REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	April 1996	Professional Paper

4. TITLE AND SUBTITLE

ASSURACON: THE ASSURED ATM CONNECTION

5. FUNDING NUMBERS

PR: CH99 or SY83
PE: 0602232N
WU: DN305458

6. AUTHOR(S)

T. Mattoon

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Naval Command, Control and Ocean Surveillance Center (NCCOSC)
RDT&E Division
San Diego, CA 92152–5001

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Office of Naval Research
800 North Quincy Street
Arlington, VA 22217–5660

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

Development of a security device for assuring ATM communications from a trusted workstation is described in the context of a comprehensive workstation security solution. Patterned after a STU-III device that has evolved into a secure front-end for a trusted multi-media workstation, the ASSURACON design provides a low cost, high performance multi-level secure device that supports both secure and non-secure ATM streams. The emergence of ATM communications capability, the availability of CMW technology and the development of multi-media teleconferencing applications bring together opportunities for military system developers to impart communications assurance into CMW platforms that support multi-media teleconferencing. Advances in system engineering and exploitation of new operational paradigms are helping position the role of multi-media teleconferencing for the military user to support voice, video, file transfer, display export, and related applications. This paper describes the development of a high performance cell stream security device that supports a comprehensive workstation security solution.

Published in *Proceedings of MILCOM 95*, Nov 5, 1995.

14. SUBJECT TERMS

Mission Area: Communications Security
Workstation Security
ASSURACON
ATM Streams
Cell Stream Security Device

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	SAME AS REPORT

21a. NAME OF RESPONSIBLE INDIVIDUAL	21b. TELEPHONE *(include Area Code)*	21c. OFFICE SYMBOL
T. Mattoon	(619) 553–6749	Code 4122

ASSURACON: The ASSURed Atm CONnection

Tom Mattoon
Naval Command, Control and Ocean Surveillance Center
Research, Development, Test and Evaluation Division
49180 Transmitter Road Room 2
San Diego, CA 92152-7341
31 Oct. 1994

Abstract

Development of a security device for assuring ATM communications from a trusted workstation is described in the context of a comprehensive workstation security solution. Patterned after a STU-III device that has evolved into a secure front-end for a trusted multi-media workstation, the ASSURACON design provides a low cost, high performance Multi-Level Secure device that supports both secure and non-secure ATM streams. The emergence of ATM communications capability, the availability of CMW technology and the development of Multi-Media Teleconferencing applications bring together opportunities for military system developers to impart communications assurance into CMW platforms that support Multi-Media Teleconferencing. Advances in system engineering and exploitation of new operational paradigms[1] are helping position the role of Multi-Media Teleconferencing for the military user[2] to support voice, video, file transfer, display export and related applications. This paper describes the development of a high performance cell stream security device that supports a comprehensive workstation security solution.[3]

1. Background

Development of packet encryption service for a trusted workstation is a current topic of research at NCCOSC/NRaD (Naval Command, Control and Ocean Surveillance Center/Research, Development, Test and Evaluation Division) in San Diego California[4]. The effort to produce a packet encryption peripheral for a trusted workstations prompted broadening the concept to producing an encryption *subsystem* for the trusted workstation. The convergence of the ALLPOWER [3] design with efforts at the National Security Agency (NSA) and at Naval Research Laboratory (NRL) to produce a high performance, key agile ATM encryption solution (presumably for *server* applications) illuminated the need for a lower performance, non-key agile ATM cell stream encryption device for the *user workstation*.

Research in Reference [2] demonstrated the necessity of two types of servers: Site Network Services and User Services. Site Network Services provide services to the user workstation *operating systems* for directory services, file services, key service, etc., that typically do not require encipherment service. User Services (primarily database services) serve the user *applications*. User Services require encipherment services in the network communications that the Site Network services do not usually require. Thus security services need to be selectively applied to streams of workstation activity. Implementing both Local Area Networks (LAN) and Wide Area Networks (WAN) over ATM will likewise require selective application of encipherment services.

2. Focus on the User

A revolution in the structure and operation of Navy information systems has resulted from the introduction of the Copernicus Concepts[5]. Just as Nicholas Copernicus revolutionized understanding of the movement of heavenly bodies by a suggesting a shift in viewpoint, so the Copernicus concept is changing the perspective of the operation of information systems by shifting the focus of operation from the "system" to making the "user" the center of focus. This simple, yet profound, shift in focus can step aside from the cacophony of data streams being thrust at users and empower those users to decide what activities and data resources they feel will further their mission objectives. Reference [4] adopted this same approach for implementing security services. Instead of viewing security as "something done by the underlying system," these concepts suggest

---

[1] Copernicus is the title of the C4I (Command Control Communications Computing and Intelligence) architecture being developed for the post cold war era. Reference the Phase I Requirements Definition for the Copernicus Architecture, Copernicus Project Office, Director Space and Electronic Warfare, Office of the Chief of Naval Operations, Washing, DC. 20350-2000.

[2] Command and Control Warfare Distributed Multi-level Security; INFOSEC for the C4I Warrior, V. 1.7, 22 March 1994, Second Project Report for Dr. John R. Davis, OPNAV N6H, Shane D. Deichman, Tom Mattoon, James W. Weatherford

[3] ALLPOWER The ALL PurpOse Workstation sEcurity peRipheral, Tom Mattoon, Naval Command, Control and Ocean Surveillance Center, Research, Development, Test and Evaluation Division, 49180 Transmitter Road Room 2, San Diego, CA 92152-7341, 3 May 1994.

[4] An Encryption Peripheral for Application Level Service, Tom Mattoon NRaD Code 855, 20 Apr. 1992

[5] Copernicus, op. cit..

viewing security services as "mechanisms that empower the user." In distributed military systems, the security mechanisms do indeed empower the user: authentication exerts identity and rank out to distributed destinations; confidentiality preserves the power of information in the communication process; access controls selectively share information resources; non-repudiation provides accountability etc. System engineering to apply Copernicus principals to new models of providing security services proposed placing security mechanisms and key material in the hands of users. The commercial availability of CMWs were seen as the ideal platform on which to stage these new security paradigms: A multi-level secure personal computing platform was viewed as the platform to maintain sensitivity level segregation and name-space isolation between ClearText and CipherText. A constitutive set of encipherment services was constructed of: File System encipherment (including Network File System (NFS), application level encryption (for electronic mail exchange), CD/ROM decryption, and LAN encipherment. This set of encipherment services was then promulgated as a comprehensive set of services for a user workstation, and was used to form part of the base specification for the definition of the ALLPOWER [3] design.

3. The ASSURACON Design

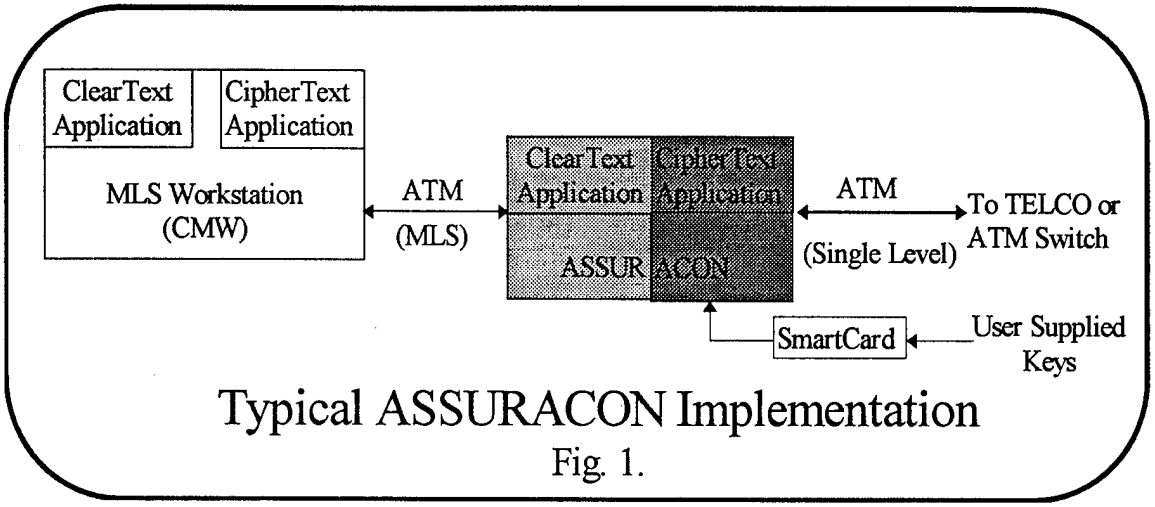
The set of requirements devised to drive the ASSURACON design were:

- STU-III like security services for circuit switched (possibly multi-destination) ATM communications.
- Basic service for securing a single ATM connection with an option for supporting multiple concurrent secure ATM connections.
- No external controls. Multi-media workstation window based controls (dial-up keyboard, voice interaction controls, hook-switch, secure services controls etc.) are required.
- Access to directory system for support in dial-up of logical entities (i.e., the user does not need to know the number just the name of the desired destination).
- Operation in heterogeneous workstation environments.
- Simple key management strategy that supports user mobility.
- Low Cost.
    - No External user controls.
    - No Key agility.
    - Moderate performance.
- Simple configuration management scheme (i.e. a simple strategy to assure that the ASSURACON is and remains correctly installed).
- Operation in Joint and Combined environments so that export controls on encipherment products are not an issue. This implies that sharing the technology and the architecture is less risky than sharing the key distribution methods.
- Inter-operability with NSA's FASTLANE product.
- Capable of operation in MLS mode between the workstation and the ASSURACON, while operating strictly single sensitivity level between the ASSURACON and the local switch or to the common carrier. This requires that all streams arriving at the ASSURACON from the workstation that are not at the sensitivity level of the common carrier or local switch be enciphered or blocked.

In order to operate in heterogeneous environments, it seemed compelling to devise a solution that functioned external to the workstation using an external (ATM) bus definition. This strategy avoided having to build a product for each workstation backplane bus and avoided the different strategies for secure communications that each workstation might implement. The ALLPOWER packing offers a tamperproof enclosure that would serve *all* workstation encipherment services. The ALLPOWER design also offers additional assurance in authenticating the user. In addition to the usual password, a Personal Computer Manufactures Communications Interface Associates (PCMCIA) security identification card[6] must also presented by the user. Since the ASSURACON design offers no external controls, and since it uses the STU-III method of operation[7], this design depends on the use of window based control objects, and upon use of the multimedia capabilities of the CMW to implement connection oriented communication services. Fig. 1 depicts a ClearText and a CipherText application in both the Workstation and in the ASSURACON. The ClearText Application in the Workstation is the application that the user invokes and uses.

[6] The Crypta Card Plus from Telequip Corporation, 18 Clinton Drive, Hollis, NH 03049.

[7] The STU-III or Secure Telephone Unit Version Three, operates by requiring the user to dial the unit like a normal telephone. The user then authenticates the destination party, inserts key material into the unit and then both participants manually actuate the secure mode of operation.



Typical ASSURACON Implementation

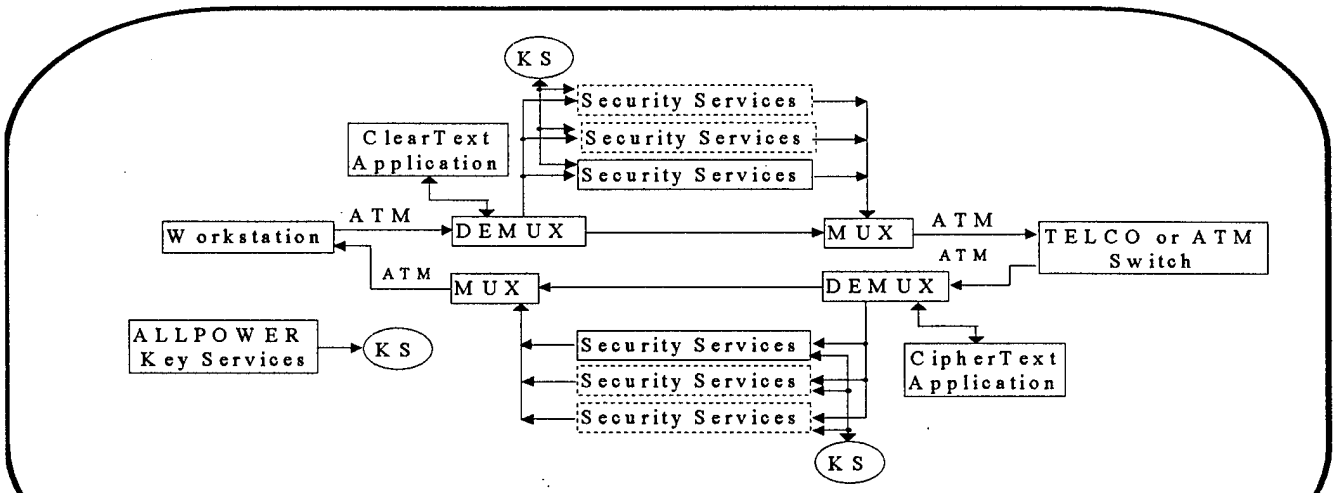
Fig. 1.

This application may or may not be adapted to interact with the ClearText Application in the ASSURACON. If it is adapted to interact with the ClearText application in the ASSURACON, then it presumably integrates the controls and the Multi-Media voice interaction support from the workstation into the application. The application would offer the keypad dialing controls or directory access methods necessary to dial-up the destination(s). The Multi-Media workstation voice facilities would then presumably capture and transmit voice communications to be sent to the destination(s) and would amplify and replay voice or sound communications for the remote participants(s). The application would also offers controls to mark a stream as requiring encipherment service. This is a critical feature with this design: Since ATM, unlike conventional analog telephone service, can support multiple service streams (using a Virtual Channel Indicator and Virtual Path Indicator, or VCI/VPI), the ASSURACON design had to decide if encipherment of all or some of the ATM streams was most useful. Since encipherment of all streams requires parallel processes or high-speed context switching with key agility, and since encipherment of all streams was not desirable (see section 1.0 Background), it is left to the user to indicate which stream(s) are to be enciphered. In this design, all ATM sessions are initiated at the sensitivity level of the ASSURACON CipherText Application (a sensitivity level that is set by site policy, since it is the sensitivity level of the site LAN). The user may then choose to initiate confidentiality (encipherment) service in order to raise (or lower) the sensitivity level of that session. The ASSURACON CipherText Application maintains a database of all active sessions, and offers a status bit that calls for encipherment for that session. The ASSURACON ClearText Application references (reads-down) into this database to determine if encipherment of a particular stream is required. This bit is controlled from either the Workstation ClearText Application (if that application has been adapted to interact with the ASSURACON) or from the Workstation CipherText Application if the ClearText Application has not been adapted.

Since applications in both the workstation and in the ASSURACON cooperate to accomplish data exchanges, both data and control flow between the Workstation and the ASSURACON. Three bi-directional data flow are defined in this design:

- Control and status between the Workstation and the ASSURACON ClearText Applications. Control flows from the Workstation for session setup and take-down and for engagement and disengagement of security services (if the application is adapted to interact with the ASSURACON). Status flows from the ASSURACON to the workstation to animate the security and session displays in the application if it has been adapted to display them.
- Data flows between the application or some Workstation hardware component and the ASSURACON. This is the service data-stream that the user designates as requiring encipherment or not.
- Control and Status between the Workstation and the ASSURACON CipherText Applications. These control and status exchanges occur if the application has not been adapted to interact with the ASSURACON, or if the user chooses to bypass the application and interact with the ASSURACON CipherText Application directly. From the CipherText Application the user can view *all* current sessions, can assure the activity of the encipherment service and observe the status of the ATM link.

Requiring the user to designate which application streams require security services is an elegant and powerful method. By following the Copernican paradigm of focusing on the



ASSURACON Functional Diagram
Fig. 2

user, the user is made responsible for circuit setup (i.e., the user places the call), the user authenticates the destination(s), the user knows the content of the information to be transferred and the user is responsible for knowing the sensitivity of the information disclosed and for disclosing this information. In order for this method to fail, *both* users must think that they have engaged secure service, and both users must be oblivious to the absence of secure service indicators available from the multi-media workstation.

Since the ATM link between the Workstation and the ASSURACON can operate in MLS mode in this design (i.e. the commingled streams can be of differing sensitivity levels), and since the ATM link between the ASSURACON and the telephone company or local switch operates a single level, it is the responsibility of the ASSURACON to provide security services (or to block) all streams that are not at the sensitivity level of the common carrier or local switch. The critical part of this design is that the ATM cells do not contain sensitivity labels, since their 53 byte size and rigid definition were not designed to contain this information. Thus sensitivity labels are appended to *streams* and these stream labels are maintained between the workstation application and the ASSURACON ClearText process. If the sensitivity level of a stream between the workstation and the ASSURACON differs from the sensitivity level of the common carrier or local switch, security services are applied to that stream, (or if resources are not available to apply security services, then that stream is blocked). Since ATM data streams that pass through the ASSURACON are either at the sensitivity level of the common carrier or local switch, or have their label transformed to the sensitive level of the common carrier or local switch by application of security services, the ASSURACON assures that all data on its 'output' side is of a single sensitivity level and that that sensitivity level is compatible with the common carrier or local switch sensitivity level (see Fig. 1).

By simplifying the design of the ASSURACON security services to not be 'key agile', the design goals of lower cost and reasonable performance can be achieved. The encipherment service is essentially a stream encipherment that is applied to the data field of ATM cells of the designated stream. Each time a cell of the designated stream arrives at the ASSURACON, the state remembered from the prior cell encipherment is maintained to continue the 'stream' encipherment. The lack of key agility is based on an assumption that most workstation users would be satisfied with a single secure stream at one time. For more sophisticated users, the ASSURACON design offers an option to support additional concurrent streams of security services. As shown in Fig. 2, the ASSURACON design offers a modular 'mother board' 'daughter board' design that will accommodate additional stream encryptor daughter boards. In this way, no key agility is required because each stream maintains its own exclusive key. The design continues to be limited by some fixed number of concurrent security streams it can support. In contrast, NSA's FASTLANE product offers key agility (i.e., keys can be put in place on a cell by cell basis), which at ATM rates is a formidable requirement. This key agility allows the FASTLANE product to support an unspecified number of concurrent secure streams, a feature that suits it well for *server* applications. The ASSURACON design supports only a single or, with optional hardware, a fixed number of secure cell streams,

which limits its applicability primarily to the user workstation.

A typical implementation of an ASSURACON device for an MLS workstation is depicted in Fig. 1. The ASSURACON design can support an untrusted workstation (such as a PC) if required, but with a limitation: The PC and the application it supports must operate at the sensitivity level of the common carrier or local switch, and the application is supports *must* be adapted to interact with the ASSURACON. Because the PC cannot be trusted to segregate processes, it cannot use the technique that the trusted workstation used of *producing* an application that interacted with the Cipher-Text side of the ASSURACON to perform circuit setup and engagement of security services on behalf of the (non-adapted) application.

4. A Comprehensive Security Solution

The ASSURACON is seen as one component in a comprehensive security solution for military workstation needs. Thus it is important to consider the architectural structure and the operational model that is used define its operational and security requirements. The architectural and operational models are still evolving to serve both the Joint and Combined environments. One proposal that is being evaluated is "INFOSEC for the C^4I Warrior" described in [2]. The main tenants of this design are:

- Don't implement security services within communication protocols. Protocols change and security services within communication protocol stacks cannot provide a complete solution.
- TELNET and FTP *user* are permissible to deploy, but FTP or TELNET *server* are ***not*** allowed. If information or services are to be made available, copy that information to some fully disclosed server for access by others. Access to military critical systems should be restricted to services that are more formally defined and that have better security features than TELNET and FTP offer.
- Structure all communications as either Multi-Media Electronic Mail (either point-to-point or multi-destination) or Multi-Media Teleconferencing, and provide separate security solutions for both services. The security solutions for Media Electronic Mail and Multi-Media Teleconferencing should be separate since the requirements for stream and block encryption differ significantly.
- Conduct client-server transactions within a peer-to-peer security arrangement.

The ASSURACON is designed to secure the communications that are structured as Multi-Media Teleconferencing, and is positioned as a component of a comprehensive workstation security solution. As described in [3], the motivation for producing a comprehensive workstation security solution is to support a common tamperproof housing, to support common key management methods for all workstation security services, to support simple configuration management, and to insure that the device is easy to use and interact with. Designing ASSURACON in light of architectural considerations, as well as system use and site configuration considerations is helpful in supporting product and user acceptance.

5. Peer-Peer Interactions

Providing system services and security services with a user focus is a new and different perspective than has been used in the military or even the commercial world. The model of operation for most military systems has been to build systems that produced information products and "pushed" these products through the communication resources to potential users. It was up to the recipients to filter incoming information and to recognize information of value. Focusing on the user shifts activity to the information consumer for most information transfers. Information exchanges are becoming structured as database exchanges. Users are provided with an increasing array of database resources and query tools to explore these information bases. Even when a "data-push" model is required, for instance in real-time database updates, or whenever a user could not be expected know of the existence of information, the focus on the user empowers the user to select among alternative information streams to bring them information they feel important in meeting their mission objectives. ATM stream type communications are well suited to peer-to-peer information exchanges that occur in real-time. Multi-Media Teleconferencing, X-Window exports, FTP and TELNET operations are ideally suited to ATM service, especially when secured by ASSURACON. Client-server exchanges are well structured to operate within the peer-to-peer security arrangements offered by ASSURACON. The "peer" at a server machine is the service administrator. No service exists as a stand-alone entity. Every service needs to offer access controls, to update its service offerings and to have its actively reviewed by an administrator who is ultimately accountable for disclosures from that data service. Implementation of ASSURACON capability bring this administrator into the security arrangements as a "peer" to the user at the client machine. The administrator at the server machine need not participate as a peer in the security arrangement on a transaction-by-transaction basis, and may instead rely on process acting on his/her behalf. The administrator is held accountable at some point to review activity at the server and to look into suspicious or inappropriate activity on that server.

6. Advanced Key Distribution Concepts

A major issue in providing security services at the user workstation is managing all aspects of key provision. It is critical that the demands on the user be minimized in whatever method is used. Policy decisions may be required on whether individuals or individuals acting in some role are to be allowed to communicate (for example military personnel must ordinarily work through the Chain of Command and are not usually allowed to interact with non-direct superiors). The method of key management is also critically important. The use of asymmetrical key management methods allows great flexibility, but requires a great deal of on-line directory support and sophisticated on-line access control methods to modulate its use. Symmetrical key methods are set-up using off-line resources and are thus much simpler to put in place. They are also much more powerful in supporting access controls and in supporting user mobility. However, it is difficult to recognize all user key requirements beforehand and to put all needed keys in place before they are needed.

Consideration of the security services that are likely to be required at a workstation, and recognition of the need to provide a common key service for all these security services, together with the need for simplicity and reliability contributed to the adoption of symmetrical key methods for the ASSURACON design.

Possession of symmetrical keys serves as a means of implementing access controls, so enforcement of *discretionary* access controls is actuated by the placement of symmetrical keys. This access control can be extended to serve as an access control to a key server that can support the distribution of asymmetric keys. Thus the use of symmetrical keys seemed the fundamental choice that would support later inclusion of asymmetrical key distribution.

The distribution method for the symmetrical keys is via an enciphered user key portfolio that is written to a smart identification card. This smart identification card must insert into the ASSURACON enclosure in order to actuate service. This smart identification card also provides a stronger user authentication than does password access alone. In this way the ASSURACON design depends on a simple, powerful key distribution method that is personalized, simple for the user to actuate and understand, allows the user to be mobile, is well suited to Joint and Combined operations and can serve key requirements for all security services at a user workstation.